Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups (New Developments of Theory of Computation and Algorithms)

AUTHOR(S):

Mizuki, Takaaki; Nishizeki, Takao

数理解析研究所講究録 1205 巻 2001 年 13-18

Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups

東北大学大学院情報科学研究科　水木敬明[1]（Takaaki Mizuki）
西関隆夫（Takao Nishizeki）
Graduate School of Information Sciences,
Tohoku University

Abstract

Suppose that there are players in two hierarchical groups and a computationally unlimited eavesdropper. Using a random deal of cards, a player in the higher group wishes to send a one-bit message information-theoretically securely either to all the players in her group or to all the players in the two groups. This can be done by the so-called 2-level key set protocol. In this paper we give a necessary and sufficient condition for the 2-level key set protocol to succeed.

1 Introduction

Suppose that there are k (≥ 2) players $P_1, P_2, \cdots, P_k$ and a passive eavesdropper, Eve, whose computational power is unlimited. Consider a graph called a *key exchange graph*, in which each vertex i represents a player P_i and each edge (i, j) joining vertices i and j represents a pair of players P_i and P_j sharing a one-bit secret key $r_{ij} \in \{0, 1\}$ that is information-theoretically secure against the eavesdropper Eve. Refer to [6] for the graph-theoretic terminology. A connected graph having no cycle is called a *tree*. If the key exchange graph is a tree, then an arbitrary player can send a one-bit message $m \in \{0, 1\}$ to all the players information-theoretically securely as follows: the player sends the message m to the rest of the players along the tree; when player P_i sends m to player P_j along an edge (i, j) of the tree, P_i computes the exclusive-or $m \oplus r_{ij}$ of m and r_{ij} and sends it to P_j, and P_j obtains m by computing $(m \oplus r_{ij}) \oplus r_{ij}$.

For $k = 2$, Fischer *et al.* give a protocol using a random deal of cards to connect the two players P_1 and P_2 with an edge, that is, to form a tree on the two players [1]. (A random deal of cards will be formally described in Section 2.1.) Fischer and Wright extend this protocol to form a tree for any $k \geq 2$; they formalize a class of protocols called the "key set protocol," the definition of which will be given in Section 2.2 [2, 5]. They also give a sufficient condition on the numbers of cards for the "key set protocol" to always form a tree. Mizuki *et al.* give a simple necessary and sufficient condition on the numbers of cards for the "key set protocol" to always form a tree [8].

On the other hand, Yoshikawa *et al.* consider the following more general problem [9]. Suppose that the k players are partitioned into two hierarchical groups, which are represented as V_1 and V_2, where $V_1 \cup V_2 = \{1, 2, \cdots, k\}$ and $V_1 \cap V_2 = \emptyset$. In the hierarchy, the group V_1 is assumed to be higher than the group V_2. Yoshikawa *et al.* wish to form, as a key exchange graph, a tree T such that the subgraph T_1 of T induced by V_1 is also a tree. Such a tree is called a *2-level tree* (for the hierarchy). Once a 2-level tree T is formed, any player in the higher group V_1 can send a one-bit message m either to all the players in V_1 or to all the players in $V_1 \cup V_2$, because both T_1 and T are connected. Yoshikawa *et al.* modify the "key set protocol" in [2, 5] so that their protocol, called a "2-level protocol," forms a 2-level tree; the formal definition of the "2-level protocol" will be given in Section 2.3. They give a sufficient condition on the numbers

[1] PRESTO, JST

of cards for the "2-level protocol" to always form a 2-level tree. However, their condition is not a necessary one, and hence it has been an open problem to obtain a necessary and sufficient condition.

In this paper, we give a necessary and sufficient condition on the numbers of cards for the "2-level protocol" to always form a 2-level tree, and hence close the open problem. Using our necessary and sufficient condition, one can easily know the minimum number of cards needed to form a 2-level tree.

2 Preliminaries

We first formally describe a random deal of cards in Section 2.1, then explain the "key set protocol" in Section 2.2, and finally explain the "2-level protocol" in Section 2.3.

2.1 Random Deal of Cards

In this subsection we formally describe a random deal of cards [4].

Let C be a set of d distinct cards which are numbered from 1 to d. All cards in C are randomly dealt to players $P_1, P_2, \cdots, P_k$ and an eavesdropper Eve. We call a set of cards dealt to a player or Eve a *hand*. Let $C_i \subseteq C$ be P_i's hand for each $1 \leq i \leq k$, and let $C_e \subseteq C$ be Eve's hand. We denote this *deal* by $\mathcal{C} = (C_1, C_2, \cdots, C_k; C_e)$. Clearly $\{C_1, C_2, \cdots, C_k, C_e\}$ is a partition of set C. We write $c_i = |C_i|$ for each $1 \leq i \leq k$ and $c_e = |C_e|$, where $|A|$ denotes the cardinality of a set A. Note that $c_1, c_2, \cdots, c_k$ and c_e are the sizes of hands held by $P_1, P_2, \cdots, P_k$ and Eve respectively, and that $d = \sum_{i=1}^{k} c_i + c_e$. We call $\gamma = (c_1, c_2, \cdots, c_k; c_e)$ the *signature* of deal $\mathcal{C}$. The set C and the signature γ are public to all the players and even to Eve, but the cards in the hand of a player or Eve are private to herself, as in the case of usual card games.

Using a random deal of cards, a protocol can make several pairs of players share a one-bit secret key, as we will explain in the succeeding subsection. A reasonable situation in which such a protocol is practically required is discussed in [3, 5], and also the reason why we deal cards even to Eve is found there.

2.2 Key Set Protocol

In this subsection we explain the "key set protocol" formalized in [2, 5].

We first define some terms. A *key set* $K = \{x, y\}$ consists of two cards x and y, one in C_i, the other in C_j with $i \neq j$, say $x \in C_i$ and $y \in C_j$. We say that a key set $K = \{x, y\}$ is *opaque* if $1 \leq i, j \leq k$ and Eve cannot determine whether $x \in C_i$ or $x \in C_j$ with probability greater than $1/2$. Note that both players P_i and P_j know that $x \in C_i$ and $y \in C_j$. If K is an opaque key set, then P_i and P_j can share a one-bit secret key $r_{ij} \in \{0, 1\}$, using the following rule agreed on before starting a protocol: $r_{ij} = 0$ if $x > y$; $r_{ij} = 1$, otherwise. Since Eve cannot determine whether $r_{ij} = 0$ or $r_{ij} = 1$ with probability greater than $1/2$, the secret key r_{ij} is information-theoretically secure. We say that a card x is *discarded* if all the players agree that x has been removed from someone's hand, that is, $x \notin (\bigcup_{i=1}^{k} C_i) \cup C_e$. We say that a player P_i *drops out* of the protocol if she no longer participates in the protocol. We denote by V the set of indices i of all the players P_i remaining in the protocol. Note that $V = \{1, 2, \cdots, k\}$ before starting a protocol.

The "key set protocol" has the following four steps.

1. Choose a player P_s, $s \in V$, as a *proposer* by a certain procedure.

2. The proposer P_s determines in mind two cards x, y. The cards are randomly picked so that x is in her hand and y is not in her hand, i.e. $x \in C_s$ and $y \in (\bigcup_{i \in V-\{s\}} C_i) \cup C_e$. Then P_s proposes $K = \{x, y\}$ as a key set to all the players. (The key set is proposed just as a set. Actually it is sorted in some order, for example in ascending order, so Eve learns nothing about which card belongs to C_s unless Eve holds y.)

3. If there exists a player P_t holding y, then P_t accepts K. Since K is an opaque key set, P_s and P_t can share a one-bit secret key r_{st} that is information-theoretically secure from Eve. (In this case an edge (s, t) is added to the key exchange graph.) Both cards x and y are discarded. Let P_i be either P_s or P_t that holds the smaller hand; if P_s and P_t hold hands of the same size, let P_i be the proposer P_s. P_i discards all her cards and drops out of the protocol. Set $V := V - \{i\}$. Return to step 1.

4. If there exists no player holding y, that is, Eve holds y, then both cards x and y are discarded. Return to step 1. (In this case no new edge is added to the key exchange graph.)

These steps 1–4 are repeated until either exactly one player remains in the protocol or there are not enough cards left to complete step 2 even if two or more players remain. In the first case the key exchange graph becomes a tree. In the second case the key exchange graph does not become a connected graph and hence does not become a tree.

Considering various procedures for choosing a proposer P_s in step 1, we obtain the class of *key set protocols.*

We say that a key set protocol *works for a signature* γ if the protocol always forms a tree as a key exchange graph for any deal C having the signature γ and for any random selection of cards x and y in step 2. Let $k \geq 2$ and $\gamma = (c_1, c_2, \cdots, c_k; c_e)$. Let W be the set of all signatures for each of which there is a key set protocol working, and let L be the set of all signatures for each of which there is no key set protocol working. A simple necessary and sufficient condition for $\gamma \in W$ has been known [2, 8]. Furthermore, a characterization of "optimal" key set protocols is given in [7].

2.3 2-Level Protocol

In this subsection we explain the "2-level protocol" given in [9].

Suppose that there are two hierarchical groups V_1 and V_2. The "2-level protocol" forms a 2-level tree, whose subgraph induced by V_1 is connected. The "2-level protocol" forms a 2-level tree in which every vertex in V_2 has degree one, that is, every vertex in V_2 is a leaf. The "2-level protocol" is obtained by slightly modifying steps 1 and 3 in the key set protocol, as follows: in step 1, a player in V_1 is always chosen as a proposer P_s; and in step 3, whenever card y is held by a player P_t in V_2, P_t drops out of the protocol even if P_t holds the larger hand than P_s. Thus the "2-level protocol" has the following four steps.

1. Choose a player P_s, $s \in V_1$, as a *proposer* by a certain procedure.

2. The proposer P_s randomly determines in mind two cards x, y so that x is in her hand and y is not in her hand. Then P_s proposes $K = \{x, y\}$ as a key set to all the players.

3. If there exists a player P_t holding y, then P_s and P_t can share a one-bit secret key r_{st}. Both cards x and y are discarded.

   (a) If $t \in V_1$, then let P_i be either P_s or P_t that holds the smaller hand; when P_s and P_t hold hands of the same size, let P_i be the proposer P_s. P_i discards all her cards and drops out of the protocol. Set $V_1 := V_1 - \{i\}$. Return to step 1.

   (b) If $t \in V_2$, then P_t discards all her cards and drops out of the protocol. Set $V_2 := V_2 - \{t\}$. Return to step 1.

4. If there exists no player holding y, that is, Eve holds y, then both cards x and y are discarded. Return to step 1.

These steps 1–4 are repeated until either exactly one player in V_1 remains in the protocol or there are not enough cards left to complete step 2 even if two or more players remain. In the first case the key exchange graph becomes a 2-level tree, in which every vertex in V_2 has degree one. In the second case the key exchange graph does not become a 2-level tree.

Considering various procedures for choosing a proposer P_s in step 1, we obtain the class of *2-level protocols.*

Without loss of generality one may assume that $V_1 = \{1, 2, \cdots, k_1\}$ and $V_2 = \{k_1 + 1, k_1 + 2, \cdots, k_1 + k_2\}$ where $k = k_1 + k_2$. One may assume that all the players in V_2 hold at least one card, i.e. $c_i \geq 1$ for all i, $k_1 + 1 \leq i \leq k_1 + k_2$. Once an edge is connected to a player in V_2 during the execution of any 2-level protocol, the player in V_2 necessarily drops out of the protocol. Therefore any player in V_2 does not need two or more cards. More precisely, there is a 2-level protocol which always forms a 2-level tree for $\gamma = (c_1, c_2, \cdots, c_{k_1}, c_{k_1+1}, c_{k_1+2}, \cdots, c_{k_1+k_2}; c_e)$ if and only if there is a 2-level protocol which always forms a 2-level tree for $\gamma = (c_1, c_2, \cdots, c_{k_1}, 1, 1, \cdots, 1; c_e)$. We thus use a *2-level signature* $\alpha = (c_1, c_2, \cdots, c_{k_1}; k_2; c_e)$ to represent a signature $\gamma = (c_1, c_2, \cdots, c_{k_1}, c_{k_1+1}, c_{k_1+2}, \cdots, c_{k_1+k_2}; c_e)$. Remember that k_2 is the number of players in V_2.

We say that a 2-level protocol *works for a 2-level signature* α if the protocol always forms a 2-level tree as a key exchange graph for any deal C having the 2-level signature α and for any random selection of cards x and y in step 2. Let $k_1 \geq 1$, $k_1 + k_2 \geq 2$, and $\alpha = (c_1, c_2, \cdots, c_{k_1}; k_2; c_e)$. One may assume without loss of generality that $c_1 \geq c_2 \geq \cdots \geq c_{k_1}$. Let W^2 be the set of all 2-level signatures for each of which there is a 2-level protocol working, and let L^2 be the set of all 2-level signatures for each of which there is no 2-level protocol working.

We say that a player P_i, $i \in V_1$, is *feasible in a 2-level signature* $\alpha = (c_1, c_2, \cdots, c_{k_1}; k_2; c_e)$ if the following condition (1), (2) or (3) holds.

(1) $c_i \geq 2$.

(2) $k_2 = 0$, $c_e = 0$, $c_i = 1$ with $i = k_1$, and $c_{k_1-1} \geq 2$.

(3) $k_1 = k_2 = 1$, $c_e = 0$, and $c_i = 1$ with $i = 1$.

We define a mapping g from the set of all 2-level signatures to $\{0, 1, 2, \cdots, k_1\}$, as follows: $g(\alpha) = i$ if P_i is the feasible player in α with the smallest hand (ties are broken by selecting the player having the largest index); and $g(\alpha) = 0$ if there is no feasible player. For example, if $\alpha = (9, 9, 8, 6, 5, 3, 2, 2, 1, 1; 2; 2)$ as illustrated in Figure 1, then $g(\alpha) = 8$. We denote $g(\alpha)$ simply by g.

Yoshikawa *et al.* give a sufficient condition for $\alpha \in W^2$ as in the following Theorem 1.

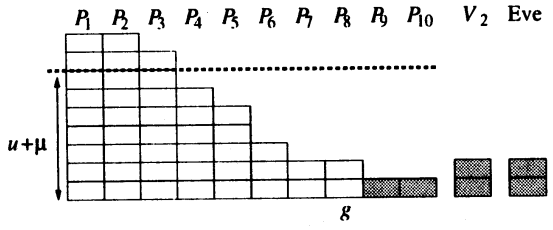

Figure 1: An illustration of $\alpha = (9,9,8,6,5,3,2,2,1,1;2;2)$.

Theorem 1 ([9]) *Let $k_1 \geq 1$, $k_2 \geq 1$, and $c_{k_1} \geq 1$. If there exists k_0 such that $0 \leq k_0 \leq k_1 - 1$ and $c_{k_1-k_0} \geq c_e + \lfloor \log_2(k_1 - k_0) \rfloor + k_0 + k_2$, then $\alpha \in W^2$.*

They prove Theorem 1 by showing that the 2-level protocol choosing the player P_g as a proposer works for any 2-level signature satisfying the condition in Theorem 1. However, their sufficient condition in Theorem 1 is not a necessary one. For example, the 2-level signature $\alpha = (9,9,8,6,5,3,2,2,1,1;2;2)$ above does not satisfy their sufficient condition in Theorem 1, while it is actually in W^2 as we will see in Section 3. Thus it has been an open problem to obtain a necessary and sufficient condition for $\alpha \in W^2$. This paper closes the open problem in Section 3, that is, provides a necessary and sufficient condition for $\alpha \in W^2$.

3 Main Results

In this section we give a necessary and sufficient condition for $\alpha \in W^2$.

Our main result is the following Theorem 2. Hereafter we define $B = \{i \mid c_i = 2,\ 1 \leq i \leq k_1\}$ and $b = \lfloor |B|/2 \rfloor$ for a 2-level signature α.

Theorem 2 *Let $k_1 \geq 1$, $k_2 \geq 1$, $c_{k_1} \geq 1$, and $g \geq 1$. Then $\alpha = (c_1, c_2, \cdots, c_{k_1}; k_2; c_e) \in W^2$ if and only if*

$$c_1 - (u+\mu) + \sum_{i=2}^{k_1} \max\{c_i - (u+\mu), 0\} \geq g - 2\mu - 1, \tag{1}$$

where

$$u = c_e + k_1 + k_2 - g \tag{2}$$

and

$$\mu = \max\{\min\{c_3 - u, b\}, 0\}. \tag{3}$$

Note that the third term in the left side of Eq. (1) is defined to be 0 when $k_1 = 1$, and that μ is defined to be 0 when $k_1 \leq 2$.

Consider again $\alpha = (9,9,8,6,5,3,2,2,1,1;2;2)$ as an example. The 2-level signature α satisfies $k_1 = 10$, $k_2 = 2$, $c_e = 2$ and $g = 8$. Thus by Eq. (2) $u = 6$. Note that u is equal to the number of shaded rectangles in Figure 1. Since $B = \{7,8\}$, $b = 1$. Since $c_3 = 8$, $u = 6$ and $b = 1$, we have $\mu = 1$ by Eq. (3). Thus $c_1 - (u+\mu) + \sum_{i=2}^{k_1} \max\{c_i - (u+\mu), 0\} = c_1 - 7 + \sum_{i=2}^{10} \max\{c_i - 7, 0\} = 5 = g - 2\mu - 1$. Therefore the 2-level signature α satisfies the condition (1) in Theorem 2, and hence $\alpha \in W^2$. Note that the left side of Eq. (1) is equal to the number of cards above the dotted line in Figure 1.

From Theorem 2 we have the following Corollary 3, which provides a necessary and sufficient condition for $\alpha \in W^2$ under a natural assumption that all players in V_1 hold hands of the same size.

Corollary 3 *Let* $k_1 \geq 1$, $k_2 \geq 1$, $c_{k_1} \geq 1$, $g \geq 1$, *and* $c_1 = c_2 = \cdots = c_{k_1}$. *Then* $\alpha \in W^2$ *if and only if*

$$c_1 \geq \begin{cases} 3 & \text{if } k_1 \geq 4,\ k_2 = 1 \text{ and } c_e = 0; \\ c_e + k_2 & \text{if } k_1 = 1; \text{ and} \\ c_e + k_2 + 1 & \text{otherwise.} \end{cases} \tag{4}$$

Theorem 1 obtained by Yoshikawa *et al.* [9] implies that a sufficient condition for $\alpha \in W^2$ is $c_1 \geq c_e + k_2 + \lfloor \log_2 k_1 \rfloor$ when $c_1 = c_2 = \cdots = c_{k_1}$. Thus our necessary and sufficient condition in Theorem 2 is much better than the sufficient condition in [9].

Due to the page limitation, we omit a proof of Theorem 2 in this extended abstract.

References

[1] M. J. Fischer, M. S. Paterson, and C. Rackoff, "Secret bit transmission using a random deal of cards," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 2, pp. 173–181, 1991.

[2] M. J. Fischer and R. N. Wright, "An application of game-theoretic techniques to cryptography," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, AMS, vol. 13, pp. 99–118, 1993.

[3] M. J. Fischer and R. N. Wright, "An efficient protocol for unconditionally secure secret key exchange," Proc. of the 4th Annual Symposium on Discrete Algorithms, pp. 475–483, 1993.

[4] M. J. Fischer and R. N. Wright, "Bounds on secret key exchange using a random deal of cards," J. Cryptology, vol. 9, pp. 71–99, 1996.

[5] M. J. Fischer and R. N. Wright, "Multiparty secret key exchange using a random deal of cards," Proc. CRYPTO '91, Lecture Notes in Computer Science, Springer-Verlag, vol. 576, pp. 141–155, 1992.

[6] F. Harary, "Graph Theory," Addison-Wesley, Reading, Mass., 1969.

[7] T. Mizuki, H. Shizuya, and T. Nishizeki, "Characterization of optimal key set protocols," Proc. IFIP TCS 2000, Lecture Notes in Computer Science, Springer-Verlag, vol. 1872, pp. 273-285, 2000.

[8] T. Mizuki, H. Shizuya, and T. Nishizeki, "Dealing necessary and sufficient numbers of cards for sharing a one-bit secret key," Proc. EUROCRYPT '99, Lecture Notes in Computer Science, Springer-Verlag, vol. 1592, pp. 389–401, 1999.

[9] R. Yoshikawa, S. Guo, K. Motegi, and Y. Igarashi, "Secret key exchange using random deals of cards on hierarchical structures," Proc. ISAAC 2000, Lecture Notes in Computer Science, Springer-Verlag, vol. 1969, pp. 290–301, 2000.